Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Reporting on Border Gateway Protocol Risk Mitigation Progress	)	PS Docket No. 24-146
	)	
	)	
Secure Internet Routing	)	PS Docket No. 22-90

To: The Commission

JOINT COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION AND WISPA – THE ASSOCIATION FOR BROADBAND WITHOUT BOUNDARIES

Michael Romano
Tamber Ray
NTCA – The Rural Broadband Association
4121 Wilson Boulevard
Suite 1000
Arlington, VA 22203

Louis Peraertz
WISPA – The Association for
Broadband Without Boundaries
200 Massachusetts Ave., NW
Suite 700
Washington, DC 20001

July 17, 2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY

NTCA – The Rural Broadband Association ("NTCA") and WISPA – The Association for Broadband Without Boundaries ("WISPA") (collectively, "Associations") submit these Joint Comments in support of the Commission's overall goal of ensuring secure routing of internet traffic, while encouraging the Commission to proceed with caution give the significant impact certain of its proposals will have on Broadband Internet Access Service ("BIAS") providers, especially smaller providers. By the Commission's own estimate, compliance with the proposed Border Gateway Protocol ("BGP") management requirements would cost the smallest of BIAS providers $22,588, an amount that could be used to connect more unserved and underserved Americans. These new compliance costs would be compounded by the plethora of reporting and compliance obligations imposed upon BIAS providers over the past two years alone. If the Commission moves forward with adopting rules in this proceeding – despite concerns about the Commission's authority to do so – the Commission should strive to minimize further burdens placed on these already resource-constrained companies.

The Associations urge the Commission to take a multi-step approach to implementing BGP routing, recognizing that BIAS providers face significant but varied barriers to implementing Route Origin Authorization ("ROA"). First, for those BIAS providers that hold Internet Protocol ("IP") addresses and have registered those addresses with the American Registry for Internet Numbers ("ARIN"), creation of ROAs is a relatively simple process. These BIAS providers, however, would benefit from a targeted awareness campaign generated by the Commission to inform providers of the process. Second, for BIAS providers that lease IP addresses that were acquired prior to the ARIN's establishment, the Associations encourage the Commission to work with ARIN to facilitate a method that would allow reassigned IP address

holders to register those addresses with ARIN. Lastly, the Associations encourage the Commission to work with ARIN to make changes in the ROA registration process that would immediately identify potential misconfigurations at the time of registration that would avoid internet traffic drops due to misconfigurations during registration. Removing these obstacles to the ROA process would facilitate increased adoption of BGP by BIAS providers in support of the Commission's BGP routing goals.

The Associations take issue with the Commission's proposal to require BIAS providers to include ROA or Route Origin Verification ("ROV") in their contracts. Adopting a rule requiring such terms would not only be ineffective but would also exceed the Commission's statutory authority. None of the statutory provisions the Commission cites as bases for authority to adopt the proposed rules would allow the Commission to interfere in private contractual relationships. Moreover, small providers would likely be unable to demand such provisions be included in agreements with much larger upstream providers. Instead, the Commission's focus should be on eliminating obstacles to ROA adoption and assisting in a meaningful increase in ROA adoption through federal agencies' implementation of Internet routing secure measures.

If the Commission moves forward, the Commission should adopt measures that minimize the cost of developing and maintaining a BGP Plan. Recommended measures include creating a BGP Plan template and limiting the obligation of a BIAS provider that has implemented ROAs on at least 90% of their IP addresses to maintaining an electronic or printed copy of their ARIN account page.

To the extent the Commission ultimately adopts rules that apply differently based on a BIAS provider's Tier 1, 2 or 3 status, the Commission should ensure the Tiers are clearly defined. Importantly, the Commission should clarify that smaller providers do not become Tier

2 providers simply by having a limited number of enterprise customers that have their own public Autonomous System, or by connecting to other smaller providers.

As noted above, the Associations also question whether the Commission has legal authority to extend BGP reporting requirements to the full range of BIAS providers. The Commission should defer any final action in this proceeding until the pending legal challenges to the reimposition of Title II regulation to BIAS have been resolved in the courts. Absent final adjudication of the Commission's authority to reclassify broadband as a telecommunications service, the Commission's regulatory authority would not extend to imposing BGP reporting obligations on all BIAS providers and, thus, would fail to accomplish the Commission's goal of achieving uniform industry standards for BGP.

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Reporting on Border Gateway Protocol Risk Mitigation Progress	)	PS Docket No. 24-146
	)	
	)	
Secure Internet Routing	)	PS Docket No. 22-90

To: The Commission

JOINT COMMENTS
OF
NTCA–THE RURAL BROADBAND ASSOCIATION
AND
WISPA – THE ASSOCIATION FOR BROADBAND WITHOUT BOUNDARIES

NTCA–The Rural Broadband Association ("NTCA") and WISPA – The Association for Broadband Without Boundaries ("WISPA") (collectively, "Associations") hereby submit these comments in response to the Notice of Proposed Rulemaking ("*Notice*")[1] adopted by the Federal Communications Commission ("Commission") in the above-captioned proceeding. The Commission proposes to require all Broadband Internet Access Service ("BIAS") providers to prepare and update at least annually a confidential Border Gateway Protocol ("BGP") security risk management plan ("BGP Plan"). As proposed, the BGP Plan would "describe and attest to the specific efforts the service provider has made, and plans to undertake, to secure BGP routing [] using Resource Public Key Infrastructure ("RPKI")" as well as other methods at the provider's disposal.[2] More specifically, BIAS providers' BGP Plans would be required to include the

[1] *Reporting on Border Gateway Protocol Risk Mitigation Progress,* Notice of Proposed Rulemaking, PS Docket Nos. 24-146, 22-90, FCC 22-18 (rel. June 7, 2024).

[2] *Notice* at ¶ 3.

provider's plans to register and maintain Route Origin Authorization ("ROA") for the Internet Protocol ("IP") addresses that correspond to routes originated by the provider.[3] The Commission further proposes to require BGP Plans to include "the status of and plans" for the BIAS provider's deployment of Route Origin Validation ("ROV").[4]

The Associations support steps to strengthen Internet routing security and welcome this opportunity to continue working with the Commission to identify steps that can be taken, as well as the challenges, risks and burdens (both financially and operationally) that must be accounted for to effectively further this objective.[5] Assuming the Commission has authority to adopt the proposed rules, the Commission should be cognizant of the burdens they will place on smaller providers that may lack the resources to comply with new security obligations, especially in light of the cumulative effect of the plethora of other regulatory burdens the Commission has imposed on BIAS providers in recent years.

Discussion

I. THE COMMISSION CAN REMOVE ROADBLOCKS TO BIAS PROVIDERS' REGISTRATION OF ROAS.

Effective and meaningful implementation of secure BGP routing is a multistep process. To begin the BGP routing process, BIAS providers must first register and maintain ROAs on the

[3] *Id*.

[4] *Id*.

[5] NTCA filed Comments in response to the Notice of Inquiry issued by the FCC in the Secure Internet Proceeding and participated in the Secure Internet Routing Public Workshop hosted by the Commission on July 31, 2023. *See* Comments of NTCA–The Rural Broadband Ass'n, *Secure Internet Routing*, Notice of Inquiry, PS Docket No. 22-90 (filed Apr. 11, 2022) ("*NOI*"); Border Gateway Protocol Security Workshop, https://www.fcc.gov/news-events/events/2023/07/bgp-security-workshop.

IP addresses they originate. To monitor BIAS providers' progress in carrying out this directive, the Commission proposes to require all BIAS providers to prepare and update a BGP Plan that describes and attests to "the specific efforts they have made, and further plan to undertake, to create and maintain ROAs…."[6] In proposing this requirement, the Commission seeks to "establish a framework that provides for a more informed and effective multistakeholder consideration of BGP security issues by government and industry stakeholders ... that enables a constructive path for timely addressing issues identified as hindering the deployment of secure Internet routing methods."[7] Identifying and resolving these roadblocks will be essential to increasing ROA registrations.

As an initial matter, BIAS providers that hold IP addresses and have registered those addressees with the American Registry for Internet Numbers ("ARIN") can create ROAs directly through their online ARIN account at no additional cost and with a minimal time commitment. Accordingly, for BIAS providers in this category that have not yet registered ROAs for their IP addresses, the "roadblock" is likely merely awareness – provided methods are in place to minimize the risk of incorrectly creating ROAs that could result in dropped traffic. To furnish this awareness, the Commission should, perhaps in conjunction with ARIN, conduct outreach in a variety of venues, including webinars and industry conferences, to provide BIAS providers with awareness and instruction regarding how ROAs can improve Internet routing security and the method for establishing ROAs for IP addresses registered to the provider in ARIN.[8]

---

[6] *Notice* at ¶ 37.

[7] *Id.* at n. 128.

[8] *See id*. at ¶ 79 seeking comment on "government-led education campaign" to drive awareness and facilitate increased registration of ROAs.

A different, and more complicated, roadblock exists among BIAS providers that lease "legacy" IP addresses, or IP addresses that the IP address holder acquired prior to the establishment of ARIN. To implement BGP routing protocol in the U.S., the legacy IP addresses must be registered with ARIN and only the IP address holder can register the addresses. If the IP address holder leases rights to legacy IP addresses without first registering those addresses in ARIN, the lessee is unable to establish ROAs for those addresses.

The Commission recognizes this is a concern and points out that ARIN has referred for community consultation a request to allow reassigned address space holders to register their IP prefixes with ROAs.[9] The Associations encourage the Commission to work with ARIN to facilitate a method that would allow reassigned legacy IP address holders to register those addresses in ARIN. This is especially critical given that there are no more IPv4 addresses available from ARIN and, even if address holders created ROAs for their registered IPv6 address space, not all technologies today support IPv6. As a result, acquiring reassigned legacy IPv4 addresses is an important tool for ensuring entities will have sufficient IP address space to accommodate future needs. They must, however, be able to create ROAs if the Commission is going to subject BIAS providers to the requirements proposed in the *Notice*.[10]

Finally, the Associations urge the Commission to support ARIN's work to provide a mechanism that would immediately identify any potential misconfigurations when creating ROAs, a concern the Commission recognized in the *Notice* that has deterred some providers

[9] *Id*. at ¶ 81.

[10] ARIN maintains a waiting list for entities seeking IPv4 addresses, which are assigned based on an entity meeting identified policy requirements. *See* ARIN, IPv4 Waiting List, https://www.arin.net/resources/guide/ipv4/waiting_list/.

from registering ROAs.[11] Establishing this immediate "test" of ROA registrations would alleviate these companies' concerns that if they build their ROAs incorrectly, their Internet traffic will form a misconfiguration during the registration process.

Addressing and eliminating these obstacles would more effectively and immediately advance the Commission's goal of increased ROA adoption than requiring BIAS providers to describe "in detail" their efforts and plans for facilitating the ROA registrations in their BGP Plan.[12] The Commission is already aware of these obstacles. Identifying "efforts and plans" for facilitating ROA registrations in these instances will not in any way increase ROA adoption.

II. REQUIRING BIAS PROVIDERS TO INCLUDE ROA OR ROV TERMS IN THEIR CONTRACTS WOULD BE INEFFECTIVE AND EXCEED THE COMMISSION'S AUTHORITY.

The Commission seeks comment on whether to require BIAS providers to include terms in their current and/or future contracts, both those for the reassignment of IP addresses and those pertaining to "transit or other interconnectivity services," that would require customers to register ROAs.[13] The Commission further indirectly seeks comment on extending this contract requirement to ROV.[14] Finally, the Commission asks whether BIAS providers would select a different upstream provider if their transit or other interconnectivity contract required the downstream BIAS provider to implement ROAs or ROV.[15]

---

[11] *Id.*

[12] *Notice* at ¶ 48.

[13] *Id*. at ¶¶ 71-72.

[14] *Id*. at ¶ 73.

[15] *Id*. at ¶ 69.

The Commission refers to various bases of statutory authority for the actions proposed in the *Notice* as further discussed in Section V, below. None of these statutory provisions, however, would allow the Commission to interfere in BIAS providers' private contractual relationships by requiring contracts to contain terms or conditions related to registration of ROAs and/or implementation of ROV. The relevant statutory provisions do not unambiguously extend to these activities.[16]

In addition, imposing these requirements only on BIAS providers overlooks the fact that the Internet ecosystem is a mixture of content, hosting, and transit networks. Moreover, a large percentage of inbound traffic (and the destination for outbound traffic) is from/to IP addresses controlled by private enterprises other than BIAS providers. Attachment 1, for example, shows that the ten largest Autonomous Systems ("ASs") are cloud and content providers. As a result, the Commission would subject BIAS providers to conditions that do not apply to other IP address holders simply because the Commission concluded in the *2024 Open Internet Order* that BIAS providers fall within the agency's jurisdiction.[17]

As noted above, where BIAS providers own their IP addresses and those addresses are registered with ARIN, an instructional webinar demonstrating how to set up ROAs in ARIN, combined with assurance that doing so would not lead to dropped traffic due to misconfigurations, would likely result in a greater number of BIAS providers that have not

[16] *See, e.g., Loper-Bright Enterprises et al. v. Raimondo*, 603 U.S. ___, *slip op*. No. 22-451 at 23 (2024) ("when [a statutory] ambiguity is about the scope of an agency's own power" it is "perhaps the occasion on which abdication in favor of the agency is least appropriate").

[17] *Id*. at ¶ 100 ('With the reclassification of BIAS as a telecommunications service, the providers of such service are subject to Title II under the terms of the *2024 Open Internet Order*.").

already created ROAs doing so. But in instances where the downstream provider leases legacy IP addresses and therefore does not have authority to create ROAs for those addresses, language in a contract will not change that. Furthermore, many smaller BIAS providers have few options available for selecting upstream providers given their remote locations. When they do have a choice, their decision of which upstream provider to interconnect with is based on the cost of bandwidth, proximity of interconnect facilities, geographic diversity of connectivity (to build redundancy into paths), and business relationship, not the upstream provider's policies and practices.

Once again, therefore, language in a contract requiring one party or the other to register, or have registered, ROAs or, as applicable, ROV, will not lead to increased BGP routing security. Instead, the Commission's focus on creating a meaningful increase in ROA adoption should be to create awareness and, as needed and feasible, to provide assistance to other federal agencies to act on the National Cybersecurity Strategy's call to federal agencies to lead by example in implementing network routing security.[18] Doing so also would be consistent with the Office of Management and Budget's recent directive to federal agencies that the agencies include "enhancements to [BGP] to increase Internet routing security" in their Fiscal Year 2026 budget.[19] The U.S. Department of Commerce's National Telecommunications and Information Administration ("NTIA"), the Bureau of Economic Analysis, the Bureau of Industry and

[18] *National Cybersecurity Strategy*, March 2023, p. 24 ("The Federal Government will lead by ensuring that its networks have implemented [BGP]…."), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. *See also Notice* at ¶ 29.

[19] *Memorandum for the Heads of Executive Departments and Agencies*, M-24-24, July 10, 2024, NCS Pillar 4, https://www.whitehouse.gov/wp-content/uploads/2024/07/FY26-Cybersecurity-Priorities-Memo_Signed.pdf.

Security, the National Oceanic and Atmospheric Administration ("NOAA"), and the International Trade Administration heeded the National Cybersecurity Strategy's call by creating ROAs for NTIA's IP addresses residing on the Department of Commerce's network and creating a partnership between NTIA and NOAA N-Wave that allows ROAs to be established for all bureaus within the Department of Commerce.[20]

Importantly, the Department of Commerce's work also resulted in a model contract that other federal agencies can use to implement routing security.[21] Accordingly, federal agencies can continue this upward trend and make a significant contribution to routing security given the substantial number of IP addresses owned by these agencies.[22] These actions would have a far greater impact on routing security than requiring BIAS providers to include language in their transit and interconnect contracts requiring one of the parties to register ROAs.

III. THE COMMISSION CAN AND SHOULD ADOPT MEASURES THAT MINIMIZE THE COSTS AND BURDENS OF THE PROPOSED REQUIREMENTS.

The Commission estimates that the cost of creating and maintaining a BGP Plan would be $9,016 for the first year and possibly less in following years.[23] The Commission also

[20] The Commission similarly recognized in the *NOI* that coordinating with other federal agencies could help promote secure Internet routing. *See NOI* at ¶ 14.

[21] "U.S. Department of Commerce Implements Routing Security," *Press Release*, May 13, 2024, https://www.commerce.gov/news/press-releases/2024/05/us-department-commerce-implements-internet-routing-security.

[22] *See, e.g.*, "ASNs allocated in United States of America," WhoIS Request, https://whoisrequest.com/ip/us (listing DoD Network Information Center as the second largest holder of IP addresses in the U.S.).

[23] *Notice* at ¶ 89.

estimates, based on internal staff analysis, that the per-service provider cost to implement and maintain RPKI would range from $22,588 for the smallest service providers up to $314,380 for large service providers.[24] Even the lowest of these estimates is a considerable burden, particularly when taking into account the combined estimate of nearly $32,000 per year for small providers.

The Commission should take steps to reduce the financial and operational burdens of the requirements proposed in the *Notice* and allow BIAS providers to instead focus their financial and staff resources on actionable steps that would increase the security of their networks based on each provider's assessment and prioritization of risks. First, the Commission should create a BGP Plan template as proposed, leveraging stakeholder input in the template's development and refinement. This template could follow the example provided by the Commission for compliance with rules adopted by the Commission pursuant to the Communications Assistance for Law Enforcement Act.[25] To avoid confusion, the template should specify the requirements applicable to providers other than the nine largest BIAS providers identified in the *Notice* and include only the requirements to adopt and maintain ROAs.

Second, where a BIAS provider has implemented ROAs on at least 90% of the IP addresses the provider holds, calculated by the IP addresses registered to that provider in ARIN, the provider should only be required to maintain a printed or electronic copy of their ARIN account page listing the IP addresses and status of ROAs for those addresses. This would be

[24] *See Notice* at ¶ 94.

[25] *See* CALEA System Security and Integrity (SSI) Policies & Procedures Plan – Checklist, June 2024, https://www.fcc.gov/sites/default/files/SSIPlan-Checklist-0624.pdf.

consistent with the Commission's proposal for the nine largest BIAS providers and take into account small providers' limited financial and staff resources.[26]

Third, as addressed in greater detail in Section IV below, the Commission should not require smaller providers to conduct ROV. The significant costs and burdens associated with requiring smaller providers to conduct ROV would wholly outweigh the negligible impact the requirement would have on improving internet routing security, as the vast majority of internet traffic passing through such providers originates from content or cloud providers.[27]

Additional regulatory costs and reporting obligations have the greatest impact on smaller providers because they typically have the narrowest margins. At the same time, these companies – which provide the majority of the Associations' memberships – offer the greatest potential to extend broadband service to the country's most remote unserved and underserved rural locations. For these providers, the financial and operational costs that would be necessary to comply with these various obligations may well be absorbed at the expense of new network expansion, network equipment upgrades and enhanced consumer benefits, as well as additional cybersecurity measures.

Given these potential impacts, the Commission should be especially cognizant when considering further action in this proceeding that BIAS providers are already subject to a broad array of reporting and compliance requirements, a significant number of them adopted in just the

[26] *See Notice* at ¶ 54 (after the initial filing of their BGP Plan, "large service providers that file an attestation that they have registered and maintained ROAs covering at least 90% of originated routes for IP address prefixes under their control" do not need to file another BGP Plan with the Commission).

[27] *See* Attachment 2, showing the volume of inbound versus outbound traffic for one rural BIAS provider across a 24-hour period.

past two years. These new requirements include the Broadband Data Collection (and related challenge and verification processes), broadband labelling requirements, data breach reporting, digital discrimination compliance, and the reimposition of regulations arising from the Commission's return to reclassifying BIAS as a Title II telecommunications service. Some affected providers are also subject to a myriad of reporting and compliance obligations arising from participation in Universal Service Fund and other federal and state funding programs. Cumulatively, these obligations pose a considerable burden. The Commission now proposes additional unfunded mandates that will disproportionately burden smaller providers – harms that can be mitigated by adopting the Associations' recommendations.

IV. THE COMMISSION MUST CLEARLY IDENTIFY ENTITIES THAT WOULD BE SUBJECT TO NEW REQUIREMENTS AND REFRAIN FROM BURDENING SMALLER PROVIDERS WITH REQUIREMENTS THAT WOULD HAVE LITTLE IMPACT ON ACHIEVING THE COMMISSION'S STATED GOALS.

The *Notice* proposes to require all BIAS providers' BGP Plan to "describe, to the extent applicable, any contractual requirements a service provider may have for upstream third-parties to provide ROV filtering for incoming routes."[28] The *Notice* also seeks comment on requiring Tier 2 providers to attest that they are implementing ROV filtering in their peering relationships with other Tier 2 providers, and have contractual relationships with Tier 1 providers that require Tier 1 providers to perform ROV filtering on traffic being terminated to the Tier 2 provider.[29] The *Notice* further seeks comment on "circumstances where Tier 2 service providers need not provide ROV support for clients that participate in BGP routing."[30]

[28] *Id*. at ¶ 50.

[29] *Id*. at ¶ 51.

[30] *Id*.

In making these proposals, the Commission does not clearly distinguish between or define, "Tier 2 providers," and "upstream third-parties," leaving the Associations to question the obligations that would apply to their members. The Associations urge the Commission to clarify these definitions and ensure that smaller providers are not required to implement ROV.

A. The Commission Must Clearly Define Relevant Providers.

As an initial matter, the *Notice* is unclear on the meaning of "upstream third-parties." For instance, the *Notice* alternately refers to "upstream third-parties," "Tier 2 providers," "medium service providers," and "providers other than the largest service providers." The *Notice* is unclear which of these different types of providers constitutes "upstream third-parties." Furthermore, if "upstream third-parties" is equivalent to "Tier 2 providers," the Commission must provide a clear definition of such providers. Notwithstanding the Associations' stated opposition in Section II to requiring BIAS providers to negotiate specific terms with upstream providers, the Associations point out that absent a clear definition of upstream third-parties, Tier 3 providers would not be able to identify what contractual provisions they have with respect to ROV filtering nor would upstream third-parties have notice that the Commission expects such providers to conduct ROV filtering.

Further, requiring Tier 3 providers to include language in their BGP Plan that describes any contractual provisions for their upstream provider to conduct ROV on these small providers' IP addresses does not provide any value when measuring RPKI implementation. Rather, requiring this language would simply add time and cost to providers without any benefit to the Commission's objective.

B. In Clarifying Definitions Of Providers, The Commission Should Ensure That Smaller Providers Are Not Required To Provide ROV.

When defining which upstream, or perhaps Tier 2, providers the Commission anticipates should provide ROV, as well as "ROV support for clients," the Commission should be mindful of the cost and complexity of implementing ROV in addition to the risk of disrupting Internet traffic if there happens to be any misconfiguration of IP addresses along the way. ROV involves much more than simply selecting registered IP addresses in ARIN. As the Commission acknowledges, some providers already have concerns regarding the risk of misconfiguring, and therefore dropping, Internet traffic when creating ROAs.[31] When implementing ROV, the concern and risk increase exponentially. ROV also is not a one-time effort but rather requires ongoing monitoring and the personnel resources to install, configure, and maintain the server that is performing ROV. Requiring smaller broadband providers to implement ROV would have little impact on routing security as these providers' Internet traffic routes through larger transit providers for communication across the Internet.

Taking the risk versus reward approach into account, the Associations ask the Commission to clarify that smaller providers do not become Tier 2 providers simply by having a limited number of customers who have their own public AS or by connecting to other smaller providers. Doing so would fit within the Commission's definition of Tier 3 providers as "one that 'strictly purchases Internet transit' and is 'primarily engaged in delivering Internet access to end customers.'"[32]

---

[31] *Id*. at ¶ 81.

[32] *Id*. at n. 127.

Further, establishing ROV only for the IP addresses of those limited number of customers that have their own AS would add complexity and may not even be feasible. Instead, if the Commission were to classify these providers as Tier 2 providers that would then be required to implement ROV, those providers would need to maintain routing tables and validate every route to ensure there is no misconfiguration. As one report described, "ROV is the application of RPKI to validate the authenticity for BGP announcements by using ROAs. When a router receives a BGP announcement, [the router] can use ROV to determine whether there is a prefix origin hijacking by checking the prefix and the origin ASN of the BGP announcement against ROA records in RPKI repositories."[33] If each time a BGP route change is presented to a router from an upstream provider, the BGP router must access a repository, verify that the ROA covers the IP prefix being announced, and compare the AS of the ROA to verify that the route is correct, the router may require additional processing and memory capabilities. Additionally, router manufacturers may see ROV as an add-on module that will require activation and support agreements. Finally, the router would either need to accommodate full routing tables, which could require the provider to purchase more capable routing equipment at a significant expense, have technology capable of performing RPKI authentication apart from the core router.[34]

To be clear, the Associations recognize that ROV filtering is an important component of secure BGP routing; however, the Commission must clearly identify and define "Tier 2," "Tier

[33] *See* Lancheng Qin *et al*, "Understanding Route Origin Validation (ROV) Deployment in the Real World and Why MANRS Action 1 Is Not Followed," Network and Distributed System Security (NDSS) Symposium 2024, Feb. 26 - March 1, 2024, San Diego, CA. p. 2, https://www.ndss-symposium.org/wp-content/uploads/2024-214-paper.pdf.

[34] *See, e.g.*, Finnegan, Kenneth, "Standalone BGP Origin Validation with RPKI," https://arista.my.site.com/AristaCommunity/s/article/bgp-origin-validation-rpki.

3" and "upstream third-parties" so that BIAS providers can be clear on their obligations. The Commission should ensure that smaller providers do not become Tier 2 providers, subject to costly and unnecessary ROV requirements, simply by having a limited number of customers who have their own public AS or by connecting, but not providing transit to, other smaller providers.

V. THE LEGAL AUTHORITY TO EXTEND BGP REPORTING REQUIREMENTS TO THE FULL RANGE OF BIAS PROVIDERS IS UNCLEAR, AT BEST.

In the *Notice*'s brief discussion of the Commission's statutory authority to implement new BGP planning and reporting requirements, the Commission relies heavily on the recent reimposition of Title II regulation across the full range of companies providing BIAS as a foundational basis for the new requirements.[35] Given the weak support for the proposed regulations provided by several of the other specific statutory provisions upon which the Commission also relies to assert this authority, however – including Section 303(b) of the Communications Act[36] and Section 706 of the Telecommunications Act of 1996[37] – the Commission should at a minimum defer any final action in this proceeding until the currently pending legal challenges to the *2024 Open Internet Order* have been resolved in the courts.[38] If

[35] *Notice* at ¶ 100 ("With the reclassification of BIAS as a telecommunications service, the providers of such services are subject to Title II under the terms of the 2024 Open Internet Order"), *citing Safeguarding and Securing the Open Internet*, WC Docket No. 23-320, FCC 24-52, Ruling, Order, Report and Order, and Order on Reconsideration, at ¶¶ 28-29 (rel. May 7, 2024) ("*2024 Open Internet Order*").

[36] *See Notice* at ¶ 101, *citing* 47 U.S.C. § 303(b).

[37] *See Notice* at ¶ 102, *citing* 47 U.S.C. §1302.

[38] *See In Re: MCP No. 185; Open Internet Rule (FCC 24-52); Ohio Telecom Association, et al. v F.C.C.,* Nos. 24-7000 (lead), 24-3449, 24-3450, 24-3497, 24-3508, 24-3510, 24-3511, 24-3519, and 24-3538 (6th Cir. 2024).

the *2024 Open Internet Order* is remanded, limited, or vacated entirely, the thin rationale for imposing broad new reporting obligations would likely evaporate, leaving the Commission without a clear legal basis to impose across-the-board requirements.

As a practical matter, if the Commission were only able to impose the new requirements upon certain segments of the BIAS marketplace, then a key underlying premise of the proposed regulation – establishing BGP planning and reporting criteria applicable to all BIAS providers to facilitate establishment of more uniform industry standards – would be beyond the Commission's legal authority. This is so due to the very weak statutory rationale supporting extension of these requirements to broadband-only ISPs and others that do not operate as traditional telecommunications service providers, absent Title II reclassification.

Section 303(b) of the Act, for example, provides the Commission only the authority to generally "prescribe the *nature* of the service to be rendered," and contains no provisions that could support agency mandates with respect to specific transmission protocols.[39] The Commission's rationale for including this statutory provision as authority for imposing BGP requirements rests on the Commission's tentative conclusion that this language somehow encompasses "regulations that promote the security and reliability of wireless networks" even though the statute is silent on such objectives.[40] From the perspective of a wireless network, internet protocol is merely payload, the radio component is entirely agnostic as to protocols and machinations that occur within the wireline information services whose traffic is carried across the wireless networks.

[39] 47 U.S.C. §303(b) (emphasis added).

[40] *See Notice* at ¶ 101.

In addition, the central purpose of Section 706 of the 1996 Act is to "encourage the deployment … of advanced telecommunications capability" using tools such as "regulatory *forbearance*, measures that *promote competition* in the local telecommunications market, or other regulating methods that *remove barriers* to infrastructure investment."[41] In short, the intent of the statute is both to assess and to promote the availability of high-speed broadband access through the removal of regulatory and other barriers to competition, not to authorize the prescription of new administrative obligations that may discourage new investment and deployment.

Finally, the *2024 Open Internet Order* applies only to BIAS providers that offer services within the United States, while the internet is global and beyond the scope of either the *2024 Open Internet Order* or the instant *Notice*. Applying BGP in this limited fashion will not achieve the Commission's goals or be effective in securing internet routing.

Accordingly, absent final adjudication establishing the permissibility of the renewed application of the Title II regulatory scheme to all BIAS providers, the Commission's regulatory authority would not extend to imposing new BGP reporting obligations on all such providers. Thus, the Commission should not adopt final rules in this docket before these core legal issues have been resolved.

[41] 47 U.S.C. § 1302(a) (emphases added).

VI. CONCLUSION

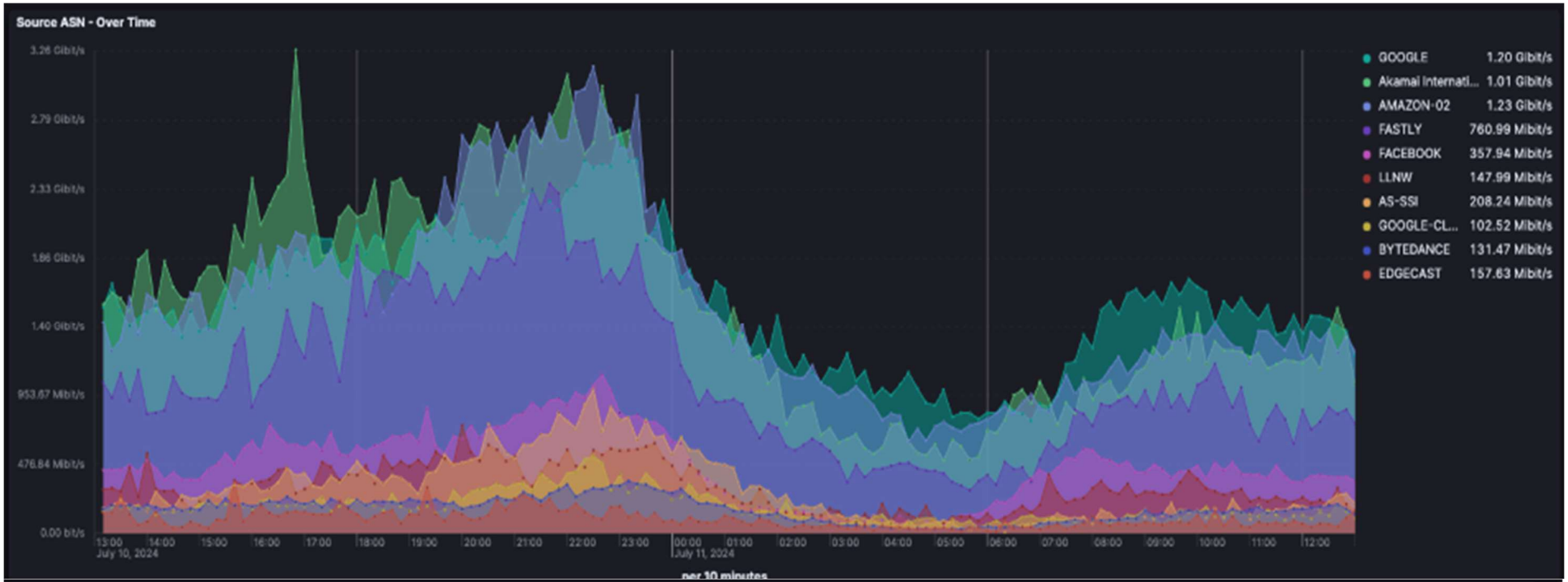
Based on the foregoing, the Associations recommend the Commission focus the current initiative on removing obstacles that interfere with BIAS providers' ability to register ROAs and refrain from imposing time consuming and costly burdens on smaller BIAS providers.

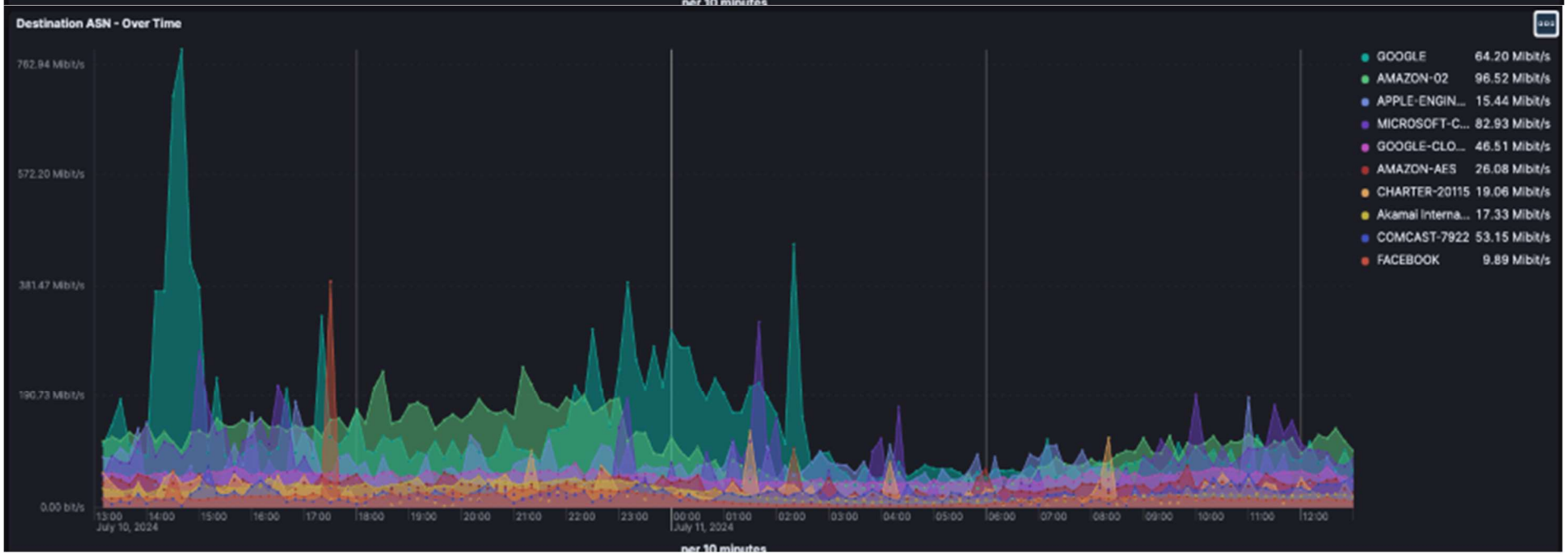
Respectfully submitted,

By: */s/ Michael Romano*
Michael Romano
Tamber Ray
NTCA – The Rural Broadband Association
4121 Wilson Boulevard
Suite 1000
Arlington, VA 22203

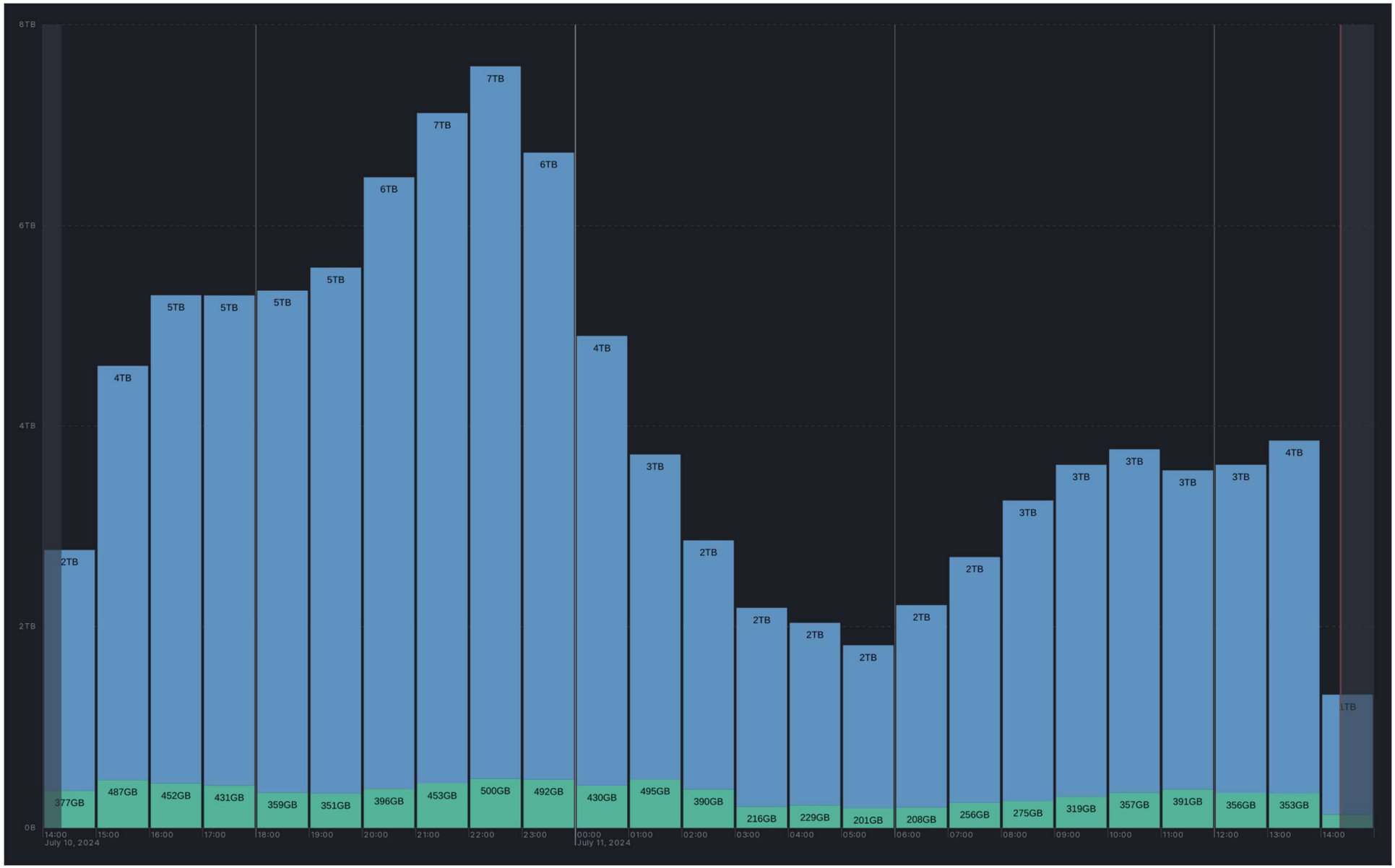
By: */s/ Louis Peraertz*
Louis Peraertz
WISPA – The Association for
Broadband Without Boundaries
200 Massachusetts Ave., NW
Suite 700
Washington, DC 20001

Attachment 1 – Source and Destination ASNs – July 11, 2024





Attachment 2 – Inbound vs. Outbound Traffic for One Rural ISP – July 11, 2024



Blue = Inbound Traffic from Rural ISP by hour for 24 hours

Green = Outbound Traffic to Rural ISP by hour for 24 hours

Submit a Standard Filing

FILING — REVIEW — 3 CONFIRMATION

Proceeding(s):	24-146, 22-90
Confirmation #:	2024071773474926
Submitted:	Jul 17, 2024 4:10:19 PM
Status:	RECEIVED
Name(s) of Filer(s)	NTCA – The Rural Broadband Association, WISPA – The Association for Broadband Without Boundaries
Law Firm(s)	
Attorney/Author/Submitter Name(s)	Michael Romano, Louis Peraertz
Primary Contact Email	scoran@lermansenter.com
Type of Filing	COMMENT
File Number	
Report Number	
Bureau ID Number	
Address of	Filer
Address	4121 Wilson Boulevard, Suite 1000, Arlington, VA, 22203
Email Confirmation	Yes

SUBMIT ANOTHER

For assistance with using ECFS, please contact the ECFS Help Desk at 202-418-0193 or via email at ECFSHelp@fcc.gov.

USA.gov